Enhanced Level of Security using DNA Computing Technique with Hyperelliptic Curve Cryptography

P.Vijayakumar[1], V.Vijayalakshmi[2], G.Zayaraz[3]

[1] Research Scholar, Department of ECE, Pondicherry Engineering College, Puducherry

[2] Assistant Professor, Department of ECE, Pondicherry Engineering College, Puducherry

[3] Associate Professor, Department of CSE, Pondicherry Engineering College, Puducherry

Email : [1]vijayrgcet@gmail.com;[2]vvijizai@pec.edu;[3]gzayaraz@pec.edu

Abstract - **Hyperelliptic Curve Cryptography (HECC) is a Public Key Cryptographic technique which is required for secure transmission. HECC is better than the existing public key cryptography technique such as RSA, DSA, AES and ECC in terms of smaller key size. DNA cryptography is a next generation security mechanism, storing almost a million gigabytes of data inside DNA strands. Existing DNA based Elliptic Curve Cryptographic technique require larger key size to encrypt and decrypt the message resulting in increased processing time, more computational and memory overhead. To overcome the above limitations, DNA strands are used to encode the data to provide first level of security and HECC encryption algorithm is used for providing second level of security. Hence this proposed integration of DNA computing based HECC provides higher level of security with less computational and memory overhead.**

Index Terms - **DNA Sequence, Koblitz's Method, Hyperelliptic Curve Cryptography (HECC), Elliptic Curve Cryptography (ECC).**

I. Introduction

Cryptographic techniques are broadly classified into symmetric key cryptographic techniques (DES, TDES, AES) and asymmetric key cryptographic techniques (RSA, ECC, HECC). In 1988, Koblitz proposed for the first time the use of Jacobian of a Hyperelliptic Curve (HEC) defined over a finite field to implement cryptographic protocols based on the difficulty of the discrete logarithm problem. During the past few years, Hyperelliptic Curve Cryptosystems (HECC) became increasingly popular for use in practice to provide an alternative to the widely used Elliptic Curve Cryptosystems (ECC) because of much shorter operand length than that of ECC. Recent research has shown that HECC are well suited for various software and hardware platforms and their performance is compatible to that of ECC. The reason behind for the adoption of HECC for any approach is that, for the minimal key length, HECC provides same security as ECC and RSA. HECC requires 80 bits key length compared to 1024 bits key length of RSA and 160 bits key length of ECC to provide the same level of security.

Deoxyribo Nucleic Acid (DNA) is a long linear polymer found in the core part of a cell. DNA is made up of several nucleotides in the form of double helix and it is linked with the transmission of genetic information. Each spiral strand consist of sugar phosphate as backbone and bases are connected to a complementary strand by hydrogen bonding between paired bases Adenine, thymine, guanine and cytosine.Adenine and thymine are connected by two hydrogen bonds while guanine and cytosine are connected by three. In its primitive stage, DNA cryptography is shown to be very effective. Currently, several DNA computing algorithms are proposed for cryptanalysis and Steganography problems, and they are very powerful in these areas. The concept of DNA computing combined with fields of cryptography and Steganography brings a new hope for powerful or unbreakable, algorithms [1-3].

II. Related Works

Dassen express DNA or other biological macromolecules as computing hardware. It examines the possibilities of DNA computing and opens up the general molecular computation and achieves the problems faced by DNA computing technique [4]. Watada illustrate the current state of the art of DNA computing achievements and also explain new approaches or methods contributing to solve either theoretical or application problems. DNA computing approaches a new way to solve engineering or application problems. It also provides an overview of research achievements in DNA computing and touches on the achievements of improved methods [5].Yanyan Huang analysis the development of DNA and introduces the working principle, mathematical model using DNA molecules [6]. Xing Wang applied computing theories in cryptography which will solve many hard problems successfully. He proposes a new way to use Cryptography with DNA Computing to transmit message securely and effectively. The RSA algorithm combined with DNA computing technique to encrypt and decrypt the message which requires more key size for providing same level of security as ECC [7]. Jie [8] proposes a novel design of DNA-based molecular cryptography. Random nature of DNA makes our cryptography in principle unbreakable. He presents an interesting example to encode and decode images using the proposed scheme. Kartalopoulos present a novel WDM link security methodology that borrows certain concepts of the double DNA helix. It encrypts multiple channels randomly with multiple keys to render channel monitoring by eavesdroppers virtually impossible. It also provides source authentication, finding fibre tapping as well as data-mimicking by intruders [9]. Guangzhao Cui can realize several security technologies such as encryption, Steganography, signature and authentication by using DNA molecular as information medium. He introduces the basic idea of DNA computing, and then discusses the information security technology in DNA computing [10].

DOI: 01.IJNS.4.1.6

This paper is organized as follows. This section gives introduction about DNA molecules and describes existing DNA computing based on Elliptic Curve Cryptographic scheme. Section 2 shows the algorithm for proposed DNA computing based HECC cryptographic scheme. Section 3 deals with the simulation results. The last section concludes this paper.

III. Existing DNA Computing based Elliptic Curve Cryptographic Scheme

The principle technical advantage of Elliptic Curve Cryptography over standard public key cryptography is that the keys can be shorter for the same security, saving on bandwidth and allowing more efficient cryptographic operations. The existing scheme uses ECC for encrypt and decrypt the message after encoding with DNA molecule by Koblitz's method as given in [11],[12][13]. The first level of security of this scheme is achieved by mapping the plaintext with DNA Nucleotide which is used to store large amount of data with few grams of DNA. The second level of security is achieved by encrypting the encoded plaintext using ECC encryption algorithm with lesser bit key size. This ECC based encryption requires 160 bit key size for providing higher level of security. This will cause memory and communication overhead. Hence, the existing public key cryptography requires larger key sizes thereby increasing the processing time for encryption and decryption of data. DNA computes ECC based cryptography converts plaintext into known ASCII value. So eavesdropper can easily retrieve the plaintext with the help of encoded plaintext. This imposes a serious limitation on the algorithm with added computational complexity, increased processing time and more storage requirement [14-19].

IV. Proposed DNA Computing Based HECC Cryptographic Scheme

To overcome the limitations of the existing scheme, a Hyperelliptic Curve Cryptosystem is proposed to reduce the number of bits required for generation of cipher text and also to reduce the communication and computational overhead. Hyperelliptic Curve Cryptosystem is a typical fast public key cryptosystem with high efficiency and security.

In proposed system, Hyperelliptic Curve Cryptosystem is used to provide same level of security with less computational complexity. Since HECC require less key size and less number of operations performed encrypting the message compared with ECC based cryptographic scheme. Algorithms involved to generate pair of keys (a_A, P_A), to encrypt and decrypt the message are shown below

A. Hyperelliptic Curve Cryptosystem

In 1988, Neal Koblitz proposed an expansion of Elliptic Curve cryptosystem known as Hyperelliptic Curve Cryptosystem. HECC was very much famous because of its high efficiency, shorter key length and can be easily implemented for software and hardware applications, less communication and computational overhead, less consumption power, less processing time. The security of HECC is based on the Hyperelliptic Curve discrete logarithmic problem, (i.e) k [Z_p, the computation of K=k×P where k is the private key and P is the public key of the user. So the security of HECC lies on the discrete logarithm problem in the Jacobian of the curve. Let F(q) be the finite field. Let C be the Hyperelliptic Curve equation of genus of g (g>2) over F(q) as shown in Eq.1.

$$C: y^2 + h(x)y = f(x) \qquad (1)$$

where

h(x) – polynomial of degree at most g.

f(x) is a monic polynomial of degree 2g+1.

Polynomials h(x) and f(x) are chosen which satisfied the condition as shown in Eq.2 to make Hyper Elliptic Curve for cryptosystem process.

$$y^2 + h(x)y \text{ “ } f(x) = 0 \qquad (2)$$
$$2y + h(x) = 0$$
$$h'(x)y - f'(x) = 0$$

The points are generated from the curve C which form a Jacobian group and divisor. These two key elements are useful for cryptographic scheme which is transformed from Hyperelliptic Curve [20-21]. Hyperelliptic Curve Cryptosystem consists of three processes such as key generation, encryption and decryption. These processes are named as HEC-ElG Algorithm.

B. Public Key and Private Key Generation

The following steps are followed to generate the private key and public key using divisor D and Hyperelliptic Curve.

Input : The public parameters are Hyper-Elliptic curve C, prime p and divisor D.

Output : The Public key P_A and Private key a_A.

- $a_A \in$ RN [choose a prime (a_A) at random in N];
- $P_A \leftarrow [a_A]$ D; [The P_A is represented using Mumford representation which is of the form (u(x),v(x))];
- Return P_A and a_A.

C. Encryption algorithm

To encrypt and send a message to *B*, *A* performs the following steps:

- *k* € *N* (Choose *k* as a random positive prime number in *N*);
- $Q \longleftarrow [k]D$ (*D* is the Divisor of the HEC & The form of *Q* is (*u*(*x*); *v*(*x*)));
- $P_k[k] \longleftarrow P_B$ (P_B : (*u*(*x*); *v*(*x*)) is receiver's(*Bs*) public key);
- $C_m \longleftarrow \{Q, E_m + P_k\}$ (C_m: (*u*(*x*); *v*(*x*)) is the Cipher Text to be sent).

D. Decryption algorithm

To decrypt the cipher text *Cm*, *B* extracts the first coordinate 'Q' from the cipher text then multiplies with its Private Key (a_B) and subtracts the result from the second Coordinate. This can be written as follows:

© 2013 ACEEE
DOI: 01.IJNS.4.1.6

$$\begin{aligned} E_m + kPB - a_B(Q) &= E \\ &= E_m + kP_B - k(a_B D) \\ &= m + k_{PB} \ - a_B(kD) \\ &= E_m + kP_B - kP_B \\ &= E_m. \end{aligned}$$

The Proposed DNA computing based on Hyperelliptic Curve Cryptography scheme uses HECC encryption to convert encoded DNA nucleotide into cipher text which requires only 80 bit key size for providing same level of security as ECC which reduces processing time and memory storage requirement. Proposed system provides higher level of security using HECC.

First level of security is provided by converting original text message into DNA nucleotide which can able to store millions of data in a single DNA strands. In addition this encoded nucleotide is converted into numbers as shown in Table.2.

Second level of security is provided by converting numbers into points using Koblitz method. These points act as plaintext for encryption using Hyperelliptic Curve Cryptography. The following steps are to be followed to implement the cryptographic scheme using DNA Computing with HECC as shown in Fig.1.

- *First Level of Security:* Input is given as Plaintext and converts the Plaintext into DNA nucleotide strands which has unique character by using Table.1.
- Each character of the converted DNA nucleotide is converted into Numbers.
- If Plaintext consists of the digits 0,1,2,3,4,5,6,7,8,9 then they are coded as digits itself.
- DNA Nucleotide letters are coded as shown in Table.2. These numbers are converted into points using Koblitz's method.
- *Koblitz's Method:* Pick an elliptic curve Ep (a, b).
- Elliptic Curve has N points, which are denoted as $(x_1,y_1),(x_2,y_2),\ldots\ldots.(x_n,y_n)$.
- Choose an auxiliary base parameter, for example $k = 20$. (Both parties should agree upon this)
- Each number *mk* (say), take $x = mk + 1$ and try to solve for *y*.
- If not able to solve for x= mk+1, then try x = mk +2 and then x = mk +3 until y value is obtained.

TABLE.1: CONVERSION OF PLAIN TEXT TO DNA MOLECULE

A - CCA	K - GAA	U - GTC
B - GTT	L - CGT	V - TCC
C - TTG	M - CCT	X - ACT
D - GGT	N - TCT	Y - AAA
E - TTT	O - CGG	Z - TCA
F - TCG	P - ACA	W - GCC
G - CGC	Q - CAA	
H - ATG	R - ACT	
I - AGT	S - GCA	
J - CGA	T - CTT	

TABLE.2: CONVERSION OF NUCLEOTIDE TO NUMBERS

A -10	C -20	G -30	T -40

- In practice, *y is* obtained before $x = mk + k - 1$ will hit. Then take the point (x, y). This now converts the number m into a point on the elliptic curve. In this way, the entire message becomes a sequence of points.
- *Second Level of Security:* These sequences of points are encrypted using HECC encryption algorithm to obtain the Cipher text points. These cipher text points are deciphered using HECC decryption algorithm to obtain the plaintext points.
- Consider each plaintext point (*x*, *y*) and set *m* to be the greatest integer less than (*x*-1)/*k*. Then the point (*x*, *y*) decodes as the symbol *m*.

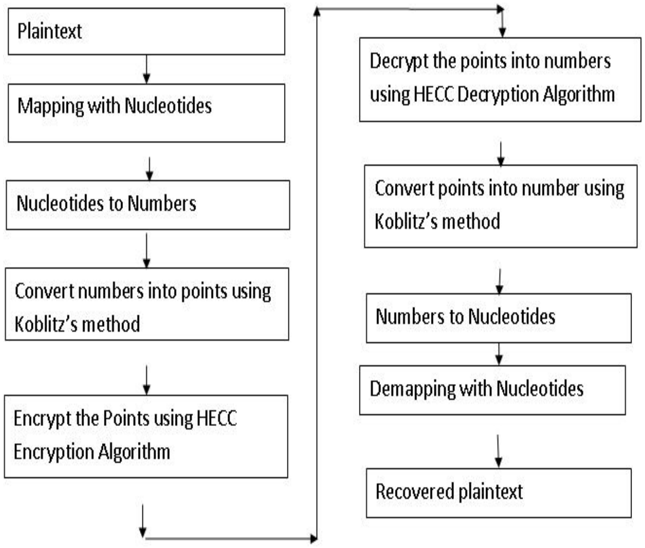
Plaintext
Mapping with Nucleotides
Nucleotides to Numbers
Convert numbers into points using Koblitz's method
Encrypt the Points using HECC Encryption Algorithm
Decrypt the points into numbers using HECC Decryption Algorithm
Convert points into number using Koblitz's method
Numbers to Nucleotides
Demapping with Nucleotides
Recovered plaintext

Fig.1 Cryptographic scheme using DNA with HECC

V. SIMULATION RESULT AND DISCUSSION

MATLAB simulation tool was used to simulate the proposed cryptographic scheme for different key size and processing time. Fig.2 shown the simulated result by comparing key size and processing time for ECC and HECC based DNA computing. From the results it was inferred that ECC takes more processing time than HECC. For key size of 100 bits, ECC takes processing time of 750ms whereas HECC takes only 150ms. From the simulated graph, it is inferred that as key size increases, the processing time for ECC increases whereas the processing time for HECC decreases.

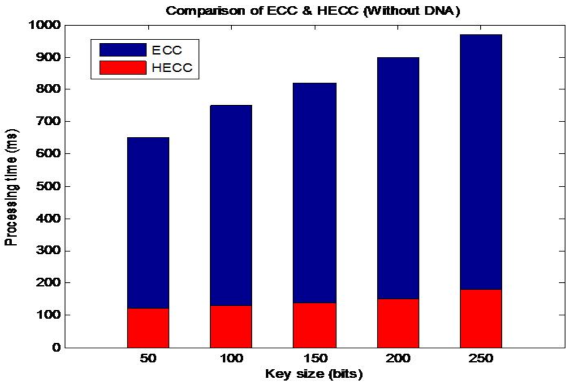

Fig.2 Key size vs processing time

DOI: 01.IJNS.4.1.6

Fig.3 shows that DNA with ECC takes more processing time than DNA with HECC. For key size of 200 bits, DNA with ECC takes the processing time of 450ms whereas DNA with HECC takes only 90ms. Thus the simulated graph shows that as the key size varies from 50 to 250, the processing time of DNA with ECC increases whereas for DNA with HECC decreases.

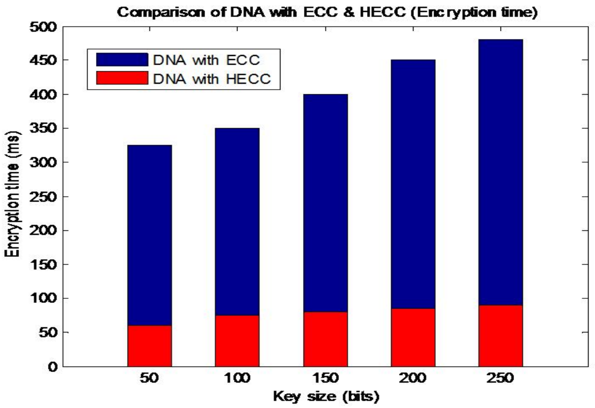

Fig.3 Key size vs encryption time

Fig.4 shows that the comparison results of proposed scheme along with the existing scheme for different message size. For message size of 1000 bits, DNA with ECC takes total processing time of 750ms whereas DNA with HECC-160 takes only 195ms. From the simulated graph, it is inferred that proposed DNA with HECC saves 550ms of processing time for 3000 bits string length than existing scheme.

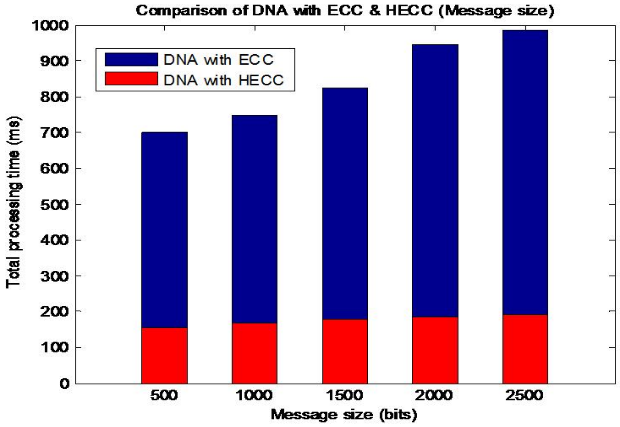

Fig.4 Message size vs total processing time

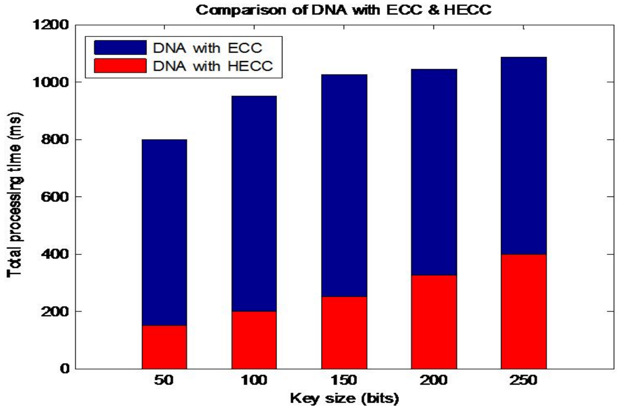

Fig.5 Key size vs total processing time

Fig.5 shows that analysis of total processing time of the proposed scheme with the existing scheme. From the simulated result, it is inferred that message size of 2000 bit, the total processing time taken for DNA with ECC scheme is 1045ms for the key size of 200 bits, whereas total processing time for proposed DNA with HECC scheme takes only 325ms seconds for 200 bits key size. Inferred results from the simulated graphs are tabulated on Table.3.

TABLE. 3: COMPARISON OF DIFFERENT KEY SIZE VS PROCESSING TIME

S. No	Phase	Existing Scheme		Proposed Scheme	
		KS(bits)	PT(s)	KS(bits)	PT(s)
1	Without DNA	100	750	100	150
2	Encryption time	200	450	200	90
3	Message size	1000	750	1000	195
4	Total Processing time (For 1000 bit Message size)	200	1045	100	325

KS- Key size; PT- Processing time

VI. CONCLUSION

This paper describes a novel cryptographic scheme by combining DNA computing theory with HECC algorithm. This proposed method offers major advantages over traditional systems such as increased speed, less memory and smaller key size. It also provides higher level of security with less key size of HECC-80 bits than ECC-160 bits. This proposed DNA based Hyperelliptic Curve cryptographic scheme can be implements in many application in wireless devices, laptop, PDA and smart cards.

REFERENCES

[1] W.Fritz and O.Hanka, "Smart Card Based Security in Locator/ Identifier-Split Architectures", *in the IEEE proceedings of* Ninth International Conference on Networks (ICN),Page(s): 194 - 200 , April 2010.

[2] Bochen Fu and Xianwei Zhang , "DNA cryptography based on DNA Fragment assembly", *in the IEEE proceedings of* 8th International Conference on Information Science and Digital Content Technology (ICIDT), Volume: 1 Page(s) : 179 - 182 , June 2012 .

[3] I.Tutanescu, C. Anton and L.Ionescu, "Elliptic Curve Cryptosystems approaches", *in the IEEE proceedings* of Information Society, Page(s): 357– 362, 2012.

[4] J.H.M.Dassen, "DNA computing" , in the IEEE proceedings of Potentials, Volume: 16 , Issue: 5, Page(s): 27 - 28 , Jan 1998.

[5] J.Watada, "DNA Computing and Its Applications", *in the IEEE proceedings of* Eighth International conference on Intelligent Systems Design and Applications, Page(s): 288 - 294 ,Nov. 2008.

[6] Yanyan Huang , "DNA computing research progress and application", *in the IEEE proceedings of* 6th International Conference on Computer Science & Education (ICCSE), Page(s): 232 – 235, 2011.

[7] Xing Wang and Qiang Zhang, "DNA computing-based cryptography", *in the IEEE proceeding of* BIC-TA '09. Fourth

DOI: 01.IJNS.4.1.6

International Conference on Bio-Inspired Computing, Page(s): 1 - 3 , Oct. 2009.

[8] Jie Chen, A DNA-based biomolecular cryptography design, *in the IEEE Proceedings of* the International Symposium on Circuits and Systems, Volume: 3, Page(s): 822 - 825, May 2003.

[9] S.V. Kartalopoulos,, "DNA-inspired cryptographic method in optical communications, authentication and data mimicking", in the IEEE proceedings of Military Communications Conference, Vol. 2 , Page(s): 774 - 779 ,Oct. 2005.

[10] Guangzhao Cui , Limin Qin, Yanfeng Wang and Xuncai Zhang, "Information Security Technology Based on DNA Computing", *in the IEEE proceedings of* International Workshop on Anti-counterfeiting, Security, Identification, Page(s): 288 – 291,April 2007.

[11] Kou Yingzhan, "Extended Fault Analysis on Elliptic Curve Cryptosystems against Repeated Doubling", *in the IEEE proceedings of* International conferences of Instrumentation,Measurement,Computer,Communication and Control, Page(s): 545 – 548, 2011.

[12] Xinxin Fan, Thomas Wollinger, and Guang Gong, "Efficient Explicit Formulae for Genus 3 Hyperelliptic Curve Cryptosystems", *in the IEEE Journal proceedings of* Information Security, Volume: 1 , Issue: 2 , Page(s): 65 – 81 , June 2007.

[13] Wen-Bing Horng ,Cheng-Ping Lee and Jian-Wen Peng," Security weaknesses of song's advanced smart card based password authentication protocol, *in the IEEE proceedings of* International Conference on Progress in Informatics and Computing(PIC),Page(s): 477–480 ,Dec2010.

[14] Xiaoyi Duan and XiuYing Li," Security of a new password authentication scheme using fuzzy extractor with Smart Card", *in the IEEE proceedings of* 3rd International Conference on Communication Software and Networks (ICCSN),Page(s): 282 - 284 , May 2011.

[15] Seoul Korea, Seo, Suk and Choi, Jin-Young , "Security analysis of smart card based password authentication schemes, *in the IEEE proceedings of* 3rd International Conference on Information Sciences and Interaction Sciences (ICIS),Page(s): 352 - 356 ,June 2010.

[16] ZhuoHao and Nenghai Yu , "A Security Enhanced Remote Password Authentication Scheme Using Smart Card", *in the IEEE proceedings of* International Symposium on Data, Privacy and E-Commerce (ISDPE), Page(s): 56 – 60, 2010.

[17] Roy S,Das, A.K. and Yu Li , "Cryptanalysis and security enhancement of an advanced authentication scheme using smart cards, and a key agreement scheme for two-party communication" *in the IEEE proceedings of* IEEE 30th International conference on Performance Computing and Communications Conference (IPCCC), Page(s): 1 - 7 ,Nov. 2011.

[18] Wen-Chung Kuo, KaiChain, Jin-Chiou Cheng and Jar-FerrYang," An Enhanced Robust and efficient Password Authenticated key agreement using smartcards", International Journal of security and its applications, Vol no.2,pp127-132,2012.

[19] R. M. Avanzi, and L. Tanja, "Introduction to Public key cryptography from Handbook of Elliptic and Hyperelliptic Curve cryptography", Henri Cohen, Gerhard Frey, Chapman and Hall/CRC, Taylor and Francis, Florida, 2006.

[20] Ramachandran Ganesan, Mohan Gobi, and Kanniappan Vivekanandan, "A Novel Digital Envelope Approach for A Secure E-Commerce Channel", *in the proceedings of* International Journal of Network Security, vol.11, No.3, PP.121-127, Nov. 2010.

[21] P. Gaudry and E. Thome."A double large prime variation for small genus Hyper Elliptic index calculus", Cryptology ePrint Archive, Report 2004/153, 2004. Available at http://eprint.iacr.org/